POLSINELLI

Protecting Privilege in the Cybersecurity Context: Applying Recent Commentary from the Sedona Conference Working Group

Updates
June 2019

Taking affirmative steps to protect sensitive IT information from disclosure during litigation is critical prior to, during and after cybersecurity incidents. Counsel and IT professionals can apply recent commentary from the Sedona Conference Working Group on Data Security and Privacy Liability to maximize the protection afforded confidential communications and documents generated in the cybersecurity context.

The Sedona Conference Working Group Commentary

The Sedona Conference Working Group on Data Security and Privacy Liability recently released draft commentary regarding the attorney-client privilege and the work product doctrine in the cybersecurity context (the "Commentary"). The Commentary provides an overview of the traditional concepts of privilege and work product protection and discusses the evolving application of those protections to communications and documents created before, during and after a cybersecurity incident. The Commentary also discusses proposals for adapting or modifying existing protections for the cybersecurity context.

The Need for Privilege in the Cybersecurity Context

Organizations generate sensitive communications and documents when proactively assessing cybersecurity threats and reacting to a data security incident. In the event litigation arises after a data security event, these documents could provide an opposing side valuable insight and evidence regarding the organization's prior knowledge of any vulnerability, decisions regarding prioritization of cybersecurity goals and potential admissions following an incident, all of which could be viewed unfavorably when analyzed in a courtroom. All personnel (including counsel and IT professionals) involved in an organization's proactive and reactive cybersecurity activities must be cognizant of the ways in which communications and documents should be protected from disclosure during litigation.

While not all information can be protected from required disclosure during litigation, organizations can take certain steps to increase the likelihood that communications and sensitive documents will be protected by the attorney/client or work product doctrine in the event of future litigation. The attorney/client privilege protects confidential communications made for the primary purpose of obtaining legal advice from a lawyer. The privilege may cover communications between a lawyer and client or between employees of the client if the primary purpose of the communication is to solicit or render legal advice. The work product doctrine protects documents prepared in anticipation of litigation, rather than for another business purpose. Both the attorney/client privilege and work product doctrine can be waived if the documents are unnecessarily disclosed to certain parties.

Practical Takeaways to Preserve Privilege in the Cybersecurity Context

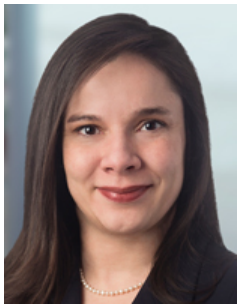
In light of the Working Group's Commentary, organizations should consider taking following steps to protect communications and documents generated before and after a data security incident:

- Involving counsel in proactive pre-incident activities, including ensuring that cybersecurity or other IT assessments are developed at the direction of counsel. Counsel should consider coupling security assessments with evaluations of ongoing regulatory requirements (e.g., the FTC Act, HIPAA, state data security laws). Counsel can also use these assessments to prioritize security controls based on legal risk and compliance obligations.
- Ensuring summaries and analysis by employees are created at the direction of, and for the purpose of assisting, counsel in rendering legal advice to the client.
- Ensuring experts, including IT vendors and forensic investigators, are retained through and for the purpose of assisting counsel in advising the client regarding their legal obligations and are not simply a substitute for the client's own information technology employees.
- Remembering that privileges are not absolute and confidential documents could still be disclosed if the privilege is waived or if opposing party can show a substantial need for the information.
- Avoiding waiver of the privilege by avoiding disclosure of assessments, forensic reports or legal advice to third-parties or to employees outside of the client's control group.

The full Commentary can be downloaded here.

For more information, contact Polsinelli's team of Privacy and Cybersecurity attorneys.

Related Contacts



Iliana L. Peters
202.626.8327

Alexander D. Boyd
816.572.4470

Related Areas

Health Care Services

HIPAA/Health Information Privacy and Security

Privacy and Cybersecurity

Technology Transactions